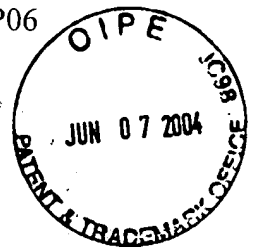
P24859.P06



IFW

GREENBLUM & BERNSTEIN, P.L.C.
Intellectual Property Causes
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

Attorney Docket No. P24859

In re application of : Paul G. BANIAK et al.

Application No. : 10/761,382 Group Art Unit: 2642

Filed : January 22, 2004 Examiner: H. Agdeppa

For : PROFILE MANAGEMENT SYSTEM INCLUDING USER INTERFACE FOR ACCESSING AND MAINTAINING PROFILE DATA OF USER SUBSCRIBED TELEPHONY SERVICES

COMMISSIONER FOR PATENTS
P.O.Box 1450
Alexandria, VA 22313-1450

Sir:

Transmitted herewith is a **Submission of Second Supplemental Declaration** in the above-captioned application.

____ Small Entity Status of this application under 37 C.F.R. 1.9 and 1.27 has been established by a previously filed statement.

____ A verified statement to establish small entity status under 37 C.F.R. 1.9 and 1.27 is enclosed.

____ An Information Dislosure Statement, PTO Form 1449, and references cited.

_X_ No additional fee is required.

_X_ Second Supplemental Declaration of Terry L. Veith Pursuant to 37 C.F.R. § 1.131.

_X_ Exhibits B & A.

The fee has been calculated as shown below:

Claims After Amendment	No. Claims Previously Paid For	Present Extra	Small Entity		Other Than A Small Entity	
			Rate	Fee	Rate	Fee
Total Claims: 14	20	0	x 9=	$	x 18=	$0.00
Indep. Claims: 1	3	0	x 43=	$	x 86=	$0.00
Multiple Dependent Claims Presented			+145=	$	+290=	$0.00
Extension Fees for ____ Month(s)				$		$0.00
			Total:	$	Total:	$0.00

____ Please charge my Deposit Account No. 19-0089 in the amount of $_____.

N/A A check in the amount of $_____ to cover the filing/extension fee is included.

_X_ The U.S. Patent and Trademark Office is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 19-0089.

_X_ Any additional filing fees required under 37 C.F.R. 1.16.

_X_ Any patent application processing fees under 37 C.F.R. 1.17, including any required extension of time fees in any concurrent or future reply requireing a petition for extension of time for its timely submission (37 C.F.R. 1.136(a)(3)).

Bruce H. Bernstein
Reg. No. 29,027 Reg. no. 33,089

P24859.A01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Paul G. BANIAK et al.
		Group Art Unit: 2642
Serial No.	:	10/761,382 (Continuation of U.S. Patent Application No. 09/050,986)
		Examiner: H. Agdeppa
Filed	:	January 22, 2004
For	:	PROFILE MANAGEMENT SYSTEM INCLUDING USER INTERFACE FOR ACCESSING AND MAINTAINING PROFILE DATA OF USER SUBSCRIBED TELEPHONY SERVICES

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313

SECOND SUPPLEMENTAL DECLARATION OF TERRY L. VIETH PURSUANT TO 37 C.F.R. §1.131

I, Terry L. Vieth, declare that:

1. I am an inventor of the subject matter recited in the claims of the present application, which is a continuation of U.S. Patent Application No. 09/050,986 (hereinafter the "parent application"), which claims priority of U.S. Provisional Patent Application No. 60/042,680. The claims of the parent application were rejected in a Final Official Action mailed on March 20, 2003. The claims pending in the present application are identical to the claims rejected in the Final Official Action mailed on March 20, 2003 in the parent application. I have personal knowledge of the facts set forth in this declaration.

2. I have previously executed a Declaration of Terry L. Vieth pursuant to 37 C.F.R. §1.131 on December 17, 2002, and a Supplemental Declaration of Terry L. Vieth

pursuant to 37 C.F.R. §1.131 on August 11, 2003. Copies of these Declarations and their attachments are attached hereto and are incorporated herein by reference in their entireties.

3. I am a member of a group that conceived, prior to October 4, 1995 (i.e., prior to the filing date of DULMAN, U.S. Patent No. 5,915,008), the profile management system that the rejection in the parent application asserts is disclosed by Dulman. From prior to October 4, 1995, the group worked diligently until the profile management system was reduced to practice.

4. The profile management system that was reduced to practice as announced by the Exhibit A submitted with the Supplemental Declaration filed in the parent application on August 20, 2003 is the same profile management system that was described in the Exhibit A submitted with the Declaration filed in the parent application on January 15, 2003, and is the same profile management system that was conceived by the group prior to October 4, 1995.

5. Exhibit B submitted herewith (with dates redacted) is a copy of a memorandum written immediately preceding the reduction to practice of the profile management system, that I authored. Exhibit B submitted herewith describes the profile management system that was reduced to practice as announced by the Exhibit A submitted with the Supplemental Declaration filed in the parent application. Accordingly, Exhibit B submitted herewith also describes the profile management system that was conceived by the group prior to October 4, 1995 as described in the Exhibit A

submitted with the Declaration filed in the parent application.

I hereby declare all statements made herein of my own knowledge are true and that all statements made herein on information and belief are believed to be true; and, further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of any issued patent.

Executed on: 5-7-4

Terry L. Vieth

P24859.A04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Paul G. BANIAK et al.	
			Group Art Unit: 2642
Serial No.	:	10/761,382	
			Examiner: H. Agdeppa
Filed	:	January 22, 2004	
For	:	PROFILE MANAGEMENT SYSTEM INCLUDING USER INTERFACE FOR ACCESSING AND MAINTAINING PROFILE DATA OF USER SUBSCRIBED TELEPHONY SERVICES	

SUBMISSION OF SECOND SUPPLEMENTAL DECLARATION

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In view of the Second Supplemental Declaration of Terry L. Vieth, Exhibit B and attachments that are submitted herewith, Applicants respectfully submit that the claims of the present application are allowable over the references applied by the Examiner in parent U.S. Patent Application No. 09/050,986. In this regard, the Second Supplemental Declaration and its attachments provide information pursuant to an agreement between Applicants' representatives and the Examiner and Supervisor of parent U.S. Patent application No. 09/050,986 in a telephone interview on October 21, 2003.

In this regard, in the above-noted telephone interview, Applicants' representatives

and the Examiner and Supervisor agreed that an Advisory Action dated September 12, 2003 would be adequately addressed by submitting information contained in the Second Supplemental Declaration and Exhibit B that accompanies these remarks. In particular, in the above-noted telephone interview, Applicants' representatives were requested to clarify the previously submitted Declaration and Supplemental Declaration filed in the parent U.S. Patent Application No. 09/050,986. Agreement was reached that the term "possession" would be replaced with the term "conceived" in a Second Supplemental Declaration. Accordingly, the attached Second Supplemental Declaration indicates that Terry L. Vieth is a "member of a group that conceived, prior to October 5, 1995 (i.e., prior to the filing date of DULMAN, U.S. Patent No. 5,915,008), the profile management system that the rejection in the parent application asserts is disclosed by Dulman".

Additionally, Applicants' representatives were requested to provide additional evidence that Exhibit A, submitted with the Supplemental Declaration of Terry L. Vieth, (i.e., the press release entitled "Southwestern Bell Introduces 'Padlock' for PC's") describes the reduction to practice of the same invention that was described in Exhibit A submitted with the Declaration of Terry L. Vieth. In this regard, Exhibit B, submitted herewith, is a memorandum authored by Terry L. Vieth immediately preceding the reduction to practice of the profile management system. The Second Supplemental Declaration of Terry L. Vieth, submitted herewith, declares that the invention described in

Exhibit B is the same invention described in the Exhibit A submitted with the Supplemental Declaration of Terry L. Vieth and Exhibit A submitted with the Declaration of Terry L. Vieth. Accordingly, each of the Exhibits (i.e., Exhibit B, Exhibit A submitted with the Supplemental Declaration of Terry L. Vieth and Exhibit A submitted with the Declaration of Terry L. Vieth), describe the same invention.

Accordingly, Applicants submit that the Declaration, Supplemental Declaration, and Second Supplemental Declaration, as well as the exhibits attached thereto, establish conception by the Applicants, prior to October 4, 1995, of the invention that the Examiner asserted is disclosed by DULMAN. Additionally, Applicants submit that the Declaration, Supplemental Declaration, and Second Supplemental Declaration, as well as the exhibits attached thereto, establish reduction to practice, with diligence from prior to October 4, 1995 until the profile management system was reduced to practice, of the profile management system that the Examiner asserted is disclosed by DULMAN.

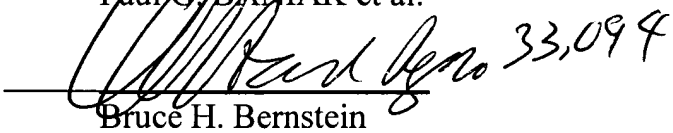
Accordingly, Applicants respectfully request an indication of the Allowability of each of the claims now pending.

P24859.A04

SUMMARY AND CONCLUSION

Should the Examiner have any questions, the Examiner is invited to contact the undersigned at the below-listed telephone number.

Respectfully submitted,
Paul G. BANIAK et al.



Bruce H. Bernstein
Reg. No. 29,027

June 7, 2004
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

DATE:
AUTHOR: Terry Vieth

EXHIBIT B

REDACTED

POSID - POSITIVE ID
SMS PROCESSING - NEW PRODUCT REQUIREMENTS

Open Issues:

1. POSID USOC/FIDS - Updated document on with confirmed USOC values. Updated document on with approved FIDs.

2. Profile Management System/PC Interface requirements

3. A USOC is sent to the SMS from SOAC as an AINID and does not contain a USOC data value. There is a default value specified in the call_variable_ref table. However, the default value specified is used in the absence of the USOC or, in the case of FIDs, the FID data. The presence of a USOC indicates to set a value associated with a call variable to be sent to SPACE. However, this value is not in a reference. A decision has been made to add a new column to the call_variable_ref table called alt_default_value which will contain the default value to use when the USOC is present on the order.

Deployment Schedule:

POSID will be deployed in Austin on , San Antonio, Houston, Dallas/Ft. Worth, St. Louis, Kansas City, Topeka, Wichita, Oklahoma City, Tulsa on , and then Little Rock on . However, as will be described further in this document, POSID requires a PC interface for customers to modify their subscription data. It has been stated that POSID will not be deployed without the PC interface, as DTMF is much too cumbersome for customers to submit large subscription data updates. Basically, the deployment of POSID is dependent on the availability of the PC interface. The PC Interface or client software will be ready , however, the PC Interface Server to SMS interface will not be available until . Subscription updates collected by the PC Server between and will be manually provisioned by the CNOC.

Product Description:

POSID provides security for access to business phone lines. POSID enables subscribers to prevent all incoming calls from being connected, except those from given Calling Party Numbers (CPNs) or Access Codes. POSID is targeted towards business customers with Computer Systems or remote access to PBX Features. POSID subscribers can create a screening list containing up to 500 Authorized CPNs. In addition, the POSID subscriber can create a second screening list containing up to 100 Access Codes. The subscriber can choose to use the Authorized CPN list, the Access Code list or a combination of both.

(The use of the access code screening list does not provide the same level of security as the CPN screening list. However, there are occasions when the CPN is not delivered, i.e., ISDN, etc.)

If the caller into the POSID equipped line is not calling from an authorized number and does not input a correct access code, then the call will be sent to a denial announcement and disconnected. If, for some reason, the ISCP is down and we cannot determine allowed CPNs or access codes, then all calls will be denied completion.

POSID Subscribers can choose to receive two reports:

- Successful Attempts Log - 100% sampling of all authorized accesses to POSID
- Unsuccessful Attempts Log - 100% sampling of all unauthorized attempts to POSID

Each report is offered weekly, monthly or both. There will be a different recurring rate for a weekly report vs. a monthly report. The SMS will receive a daily file from DRS and be responsible for producing the POSID reports.

Target Market:

The target market for POSID is any medium or large business customer that employs the public switched network as a means to provide access to its computer system(s). Southwestern Bell customers that have deployed office automation/mechanization systems, remote data access or sales force automation applications are candidates for this service. In addition, any customer that has/will be utilizing work-at-home applications could benefit from the POSID service.

Rating/USOCs/FIDs:

The POSID product will be offered with Volume Discounting. Based on the number of Working Telephone Numbers (WTNs) equipped with POSID for a given Billing Telephone Number (BTN), the POSID product will contain a different recurring rate. Basically, customers with 1-3 lines equipped with POSID would be charged one rate, customers with 4-7 lines equipped with POSID would be charged a different rate, and customers with 8 or more lines equipped with POSID would be charged with yet a different rate. There are several options available to accomplish the tiered billing approach:

1. POSID could be rated and billed at the BTN level. Each WTN equipped with POSID would contain a free POSID USOC used for provisioning purposes.

REDACTED

2. Offer three different POSID USOCs, one for each tier. Based on the number of WTNs equipped with POSID on a given BTN, the service representative would apply the correct USOC.

3. Offer a single POSID USOC which would be applied on each POSID equipped WTN. If a given BTN contains more than 3 POSID equipped WTNs, apply a negative USOC to each POSID equipped WTN which would in essence provide a discount.

4. Manually rate the POSID equipped WTNs. Apply a USOC to each POSID equipped WTN followed by the rate (one of the three tiers). The rate supplied on the service order would override the mechanical rating in CRIS.

It was decided by CRIS, Product Development, Marketing Methods, and the SMS to go with Option Number 3. SOAC will be updated to recognize the single POSID USOC and will ignore the negative POSID USOC, as the SMS is not interested in the rate.

A FID will follow the POSID USOC. The FID ASID (Account Security Identification) will contain up to 30 characters following it. The string of 30 characters can be anything and is specified by the customer. It will be used to verify the customer's identity when pin resets are requested. The FID data is not provisioned to a SPACE template and is considered a Local Only Update (LOU). For now, the ASID FID and FID data will be stored in the SMS and CRIS. The reason for storing in CRIS is to make the information available to our service representatives. This is due to EASE not having query capability to the SMS. This obviously is not secure, since basically anyone can see the information if it is in CRIS. The ASID FID data is not provisioned to SPACE on the template, but will be a Local Only Update in the SMS.

A separate non-recurring USOC will be used to reset a customer's pin number. The Pin will be sent to the SMS behind the FID RPI (Reset PIN). However, the RPI FID will be mapped in SOAC to the POSID recurring USOC. Thus, the SMS will not receive the pin reset USOC. Following the RPI FID will be the default PIN data. The default is the last 6 digits of the customer's WTN. The PIN reset USOC will be NR9SP. However, the RPI FID/FID data will be mapped to the POSID USOC (SCMBX) and the SMS will never receive the NR9SP USOC.

A new FID CARC will be created and sent to the SMS along with the USOC SCMBX. The FID data contains a customer name and telephone contact number. A PC Server application administration person will contact this name and telephone number to negotiate customer User IDs for the PC server and PC Interface software distribution. The FID data will be a minimum of 15 and maximum of 62 characters. The customer name will appear first followed by a comma and then the contact telephone number in the format NPA NXX-LINE. The FID data is not provisioned to a SPACE template and is considered a Local Only Update.

A new FID ADID will be created and sent to the SMS along with the USOC SCMBX when the WTN is a DMS100 DID Line. The value following the FID will be Y (Yes). This FID is not required and only present on a DMS100 DID line. When this FID is present (only on inward activity), the SMS will be required to then require two additional FIDs to be populated. These FIDs are phony FIDs #DIGT (DMS DID digit) and #TRNK (DMS DID trunk). The information to populate the #DIGT and #TRNK FID is located in the central office switch and can be determined by doing a QDN. When ADID is present on the inward activity, the SOAC activation request should be erred to the Software Center who would execute the QDN in the switch and populate the new phony FIDs.

The Successful Attempts Log report will appear with one of two different recurring USOCs. The report can be offered weekly or monthly. There are no FIDs associated with the report. The SMS will only receive one of the two possible USOCs as there is a single call variable in the SPACE template. The call variable contains a Y/N value and is not sensitive to whether the report is monthly or weekly. The Successful Attempts Log report weekly USOC is RS6WX and the monthly USOC is RS6MX. The SMS will only receive the RS6WX USOC. The RS6MX USOC will be mapped to RS6WX in SOAC.

The Unsuccessful Attempts Log report will appear with one of two different recurring USOCs. The report can be offered weekly or monthly. There are no FIDs associated with the report. The SMS will only receive one of the two possible USOCs as there is a single call variable in the SPACE template. The call variable contains a Y/N value and is not sensitive to whether the report is monthly or weekly. The Unsuccessful Attempts Log Report weekly USOC is RU6WX and the monthly USOC is RU6MX. The SMS will only receive the RU6WX USOC. The RU6MX USOC will be mapped to RU6WX in SOAC.

In summary, the following USOCs and FIDs will be sent to the SMS from SOAC:

- SCMBX - USOC which identifies a POSID subscriber
  RPI - FID which contains default PIN data (last 6 digits of the WTN)
  ASID - FID which contains up 30 characters used for customer validation purposes
  ADID - FID which identifies a DMS100 DID line. FID Value = Y.
  CARC - FID which identifies a customer name and contact telephone number
- RS6WX - USOC for the Weekly Successful Attempts Log Report. This USOC will also be mapped to the SMS when the RS6MX (Monthly) USOC is present on the order.
- RU6WX - USOC for the Weekly Unsuccessful Attempts Log Report. This USOC will also be mapped to the SMS when the RU6MX (Monthly) USOC is present on the order.

Both the CPN screening list and the Access Code screening list will not be provisioned via a service order. Yet, the GUI interface will have the ability to provision/modify both lists. As a result two phony FIDs used only by the SMS will be established and used to provision the embedded tables. The Access Code screening list table also contains one

comment column for each row. The CPN screening list contains two comment columns for each row. Comments can be up to 30 characters. In addition, there are two new phony FIDs associated with the DMS100 DID lines. A phony FID also has been created to provision the car_active call variable. This FID is only used to provision a number change and retain the customer's active setting. The phony FIDs are:

- #CAR1 - FID used to specify updates to the Access Code screening list
- #CM11 - FID used to specify a comment for each Access Code in the Access Code screening list
- #CAR2 - FID used to specify updates to the CPN screening list
- #CM21 - FID used to specify a comment for each CPN in the CPN screening list
- #CM22 - FID used to specify a second comment for each CPN in the CPN screening list
- #DIGT - FID used to specify the DMS DID digit
- #TRNK - FID used to specify the DMS DID trunk
- #ACTV - FID used to specify the car_active setting. Basically specify whether the service is on or off.

Service Orders:

SORD/EASE will be modified to allow for the following USOCs: SCMBX, RCRSA/RCRSB (Negative POSID USOC), RS6WX, RS6MX, RU6WX, RU6MX, NR9SP (POSID Reset PIN USOC). In addition, the FID RPI, ASID, and CARC will be allowed. When the RPI FID is present, SORD/EASE will mechanically populate the FID data with the last 6 digits of the customer's WTN. In addition, SORD will generate the ADID FID when the USOC SCMBX is present with an 'I' action code following the USOCs PLP or PLPTX (PLP and PLPTX indicate DID) and the customer is served by a DMS-100 switch.

Class of Service Restrictions:

POSID will not be offered on virtual numbers, coin class of services, or mobile, regardless of switch type. POSID will be offered to all other Business class of services.

Currently, POSID is not available on ISDN lines served from a 5ESS switch (availability planned for 1997)

For Hunting arrangements, POSID is available for Series Hunting provided each line in the Hunt group is equipped with Positive ID. For Terminal Hunting, only the lead number in the hunting arrangement needs to be equipped with Positive ID.

If a customer subscribes to POSID, the only other AIN service the customer may subscribe to is DRS.

USOCs RS6WX, RS6MX, RU6WX, RU6MX should not be allowed for customer's served by an AT&T 1A switch with 0.0 AIN software. The switch cannot determine whether the calling number is private or not. Once the AT&T 1A switch is updated to version 0.1 AIN software, the POSID reports can be offered.

Seimens (ISDN and SmartTrunk) and Ericsson switches are not supported at this time.

Following is an example of POSID Inward activity:

REDACTED

```
314 231-9999  222   WIC
C123456     1BH   AAA
-LSTG
LN     HAIRBOWS; VIETH'S
LA     603 LAKEFIELD
       /DZIP 62236
-CTL
WCO    SDM TERRY VIETH
       314 235-3659
-BILL
TAR    STL
PCL    B
IRRMA 1 3HD MON;
        MEDIA CONSULTING INC;
        ATTN;  REE PORTA
        123 MAIN;
        SUITE 42;
        ST. LOUIS, MO 63010
-RMKS
RMK    POSID INWARD EXAMPLE
-S&E
R      1BH    /TN 1504
              /PIC 0288-ATX,063090,
              070295,S/RMK ZAP
R      9ZR
R      ESM
I      SCMBX        /RPI 319999
                    /ASID FUNNYBOWS
                    /CARC DIXIE JONES;
                     314 235-9277
I      RS6WX .
I      RU6WX
$
```

Following is an example of POSID Change activity:

REDACTED

```
314 231-9999  222   WIC
C123456      1BH   AAA
-LSTG
LN     HAIRBOWS; VIETH'S
LA     603 LAKEFIELD
       /DZIP 62236
-CTL
WCO    SDM TERRY VIETH
       314 235-3659
-BILL
TAR    STL
PCL    B
-RMKS
RMK    POSID INWARD EXAMPLE
-S&E
R      1BH    /TN 1504
              /PIC 0288-ATX,063090,
              070295,S/RMK ZAP
R      9ZR
R      ESM
R      RPT2W
C      SCMBX      /ASID FUNNYBOWS
                  /CARC DIXIE JONES;
                   314 235-9277
T      SCMBX      /ASID FUNNYGIRL
                  /CARC DIXIE JONES;
                   314 235-9277
I      NR9SP      /RPI 319999
O      RS6WX
I      RS6MX
$
```

SOAC to SMS Activation Request:

Following is an example of POSID Inward Request (non-AIN customer adding POSID):

```
*C3{FT=PRE;TT=SO;OT=C;ORDNO=123456;MT=F;TRN=1;
 TSYS=SOACTS8;RSYS=SMS1;PRI=+0;WC=314231;}%
*ODR{
        DIFF=N;
        CS=1BH;
        DD=951201;
}%
*SBR{
        CTL{
                CTC=C;
                MTN=3142319999;
                MTCCC=222;
        }
        ACL{
                ACT=O;
                BTN=3142319999;
                BTNCC=222;
                MTNCC=222;
                MTN=3142319999;
                NP=N;
                SRA=603 LAKEFIELD;
                SRN=VIETH'S HAIRBOWS;
        }
        ACL{
                ACT=N;
                BTN=3142319999;
                BTNCC=222;
                MTNCC=222;
                MTN=3142319999;
                NP=N;
                SRA=603 LAKEFIELD;
                SRN=VIETH'S HAIRBOWS;
        }
}%
```

```
*RSC{
      REC{
            CTL{
                  CTC=B;
                  CTID=TN[3142319999];
            }
            ACL{
                  ACT=N;
                  CTID=TN[3142319999];
                  TN=3142319999;
                  AINS{
                        AINID=SCMBX;
                        RPI=319999;
                        ASID=FUNNYBOWS;
                        CARC=DIXIE JONES, 314 235-9277;
                  }
                  AINS{
                        AINID=RS6WX;
                  }
                  AINS{
                        AINID=RU6WX;
                  }
            }
      }
}%
```

This is an example of a POSID Change Request. Existing AIN POSID customer is modifying POSID. RPI FID is received to reset PIN. ASID FID is received to change the customer validation character string. Customer changes Report 1 from weekly to monthly. Customer retains Report 2 (weekly). Following is the example:

```
*C3{FT=PRE;TT=SO;OT=C;ORDNO=123456;MT=F;TRN=1;
 TSYS=SOACTS8;RSYS=SMS1;PRI=+0;WC=314231;}%
*ODR{
      DIFF=N;
      CS=1BH;
      DD=951201;
}%
```

```
*SBR{
        CTL{
                CTC=C;
                MTN=3142319999;
                MTCCC=222;
        }
        ACL{
                ACT=O;
                BTN=3142319999;
                BTNCC=222;
                MTNCC=222;
                MTN=3142319999;
                NP=N;
                SRA=603 LAKEFIELD;
                SRN=VIETH'S HAIRBOWS;
        }
        ACL{
                ACT=N;
                BTN=3142319999;
                BTNCC=222;
                MTNCC=222;
                MTN=3142319999;
                NP=N;
                SRA=603 LAKEFIELD;
                SRN=VIETH'S HAIRBOWS;
        }
}%
```

```
*RSC{
      REC{
            CTL{
                  CTC=C;
                  CTID=TN[3142319999];
            }
            ACL{
                  ACT=O;
                  CTID=TN[3142319999];
                  TN=3142319999;
                  AINS{
                        AINID=SCMBX;
                        ASID=FUNNYBOWS;
                        CARC=DIXIE JONES, 314 235-9277;
                  }
                  AINS{
                        AINID=RS6WX;
                  }
                  AINS{
                        AINID=RU6WX;
                  }
            }
            ACL{
                  ACT=N;
                  CTID=TN[3142319999];
                  TN=3142319999;
                  AINS{
                        AINID=SCMBX;
                        RPI=319999;
                        ASID=FUNNYGIRL;
                        CARC=DIXIE JONES, 314 235-9277;
                  }
                  AINS{
                        AINID=RS6WX;
                  }
                  AINS{
                        AINID=RU6WX;
                  }
            }
      }
}%
```

NOTE: Notice the RPI FID is not reflected in the RSCREC Old view. This is due to CRIS dropping the FID and not retaining on the CRIS customer record.

USOC/FID to SPACE Call Variable mapping:

USOC	FID	Call Variable Name
SCMBX		car
SCMBX	#ACTV	car_active
SCMBX	RPI	car_adminpin
SCMBX	#CAR1	car_emacctbl
SCMBX	#CAR2	car_emscrtbl
SCMBX	ADID	car_dmsdid
SCMBX	#TRNK	car_dmsdidtrunk
SCMBX	#DIGT	car_dmsdiddigit
RS6WX		car_report1
RU6WX		car_report2

NOTE: FIDs ASID, CARC, #CM11, #CM21, and #CM22 are not referenced here because these FIDs are local only FIDs.

SPACE Call Variables:

The following Call Variables will be contained on the SPACE template for POSID:

Call Variable Name	Type of variable	DTMF	Default	Description
car	Yes/No	No	N	POSID Subscriber indicator used by the ISCP Feature Interaction Manager (FIM) to call POSID specific service logic.
car_active	Yes/No	Yes	N	Customer controls when to activate their service.. Once turned on, the customer cannot turn off. The option to turn the service off is available to SPACE users only for troubleshooting.
car_adminpin	7 digit numstring	Yes	last 6 digits of POSID nbr	Administrator PIN
car_emacctbl	embedded tbl - 100 rows	Yes	blank list	Embedded table of authorized access codes.
car_emscrtbl	embedded tbl - 500 rows	Yes	blank list	Embedded table of CPNs authorized to complete the call.
car_report1	Yes/No	No	N	Successful attempts report option.
car_report2	Yes/No	No	N	Unsuccessful attempts report option.
car_dmsdid	Yes/No	No	N	Required if customer is a DID customer on a DMS-100 If set to yes, the following two variables must be provided.
car_dmsdidtrunk	8 digit numstring	No	00000000	Required if customer is a DID customer on a DMS-100

car_dmsdiddigit	1 digit numstring	No	7	Required if customer is a DID customer on a DMS-100

Following are POSID embedded table specifications:

Table car_emacctbl - Authorized Access Code list:

Column Name	Type of data	DTMF	Default	Description
ACCESS_CODE	Up to 7 digit numstring	Yes	0	Authorized access code or PIN specified by the POSID subscriber. Table can contain up to 100 entries.
UNIQUE_ID	3 digit numstring	No	001	Unique ID or row number generated by SPACE. Range from 001 to 100.

Table car_emscrtbl - Authorized CPN list:

Column Name	Type of data	DTMF	Default	Description
CPN	10 digit numstring	Yes	0	Authorized CPN specified by the POSID subscriber. Table can contain up to 500 entries.
UNIQUE_ID	3 digit numstring	No	001	Unique ID or row number generated by SPACE. Range from 001 to 500.

SMS to SPACE Activation Request:

```
*U4{
        trnsId=12345678901234567890,
        ft=PRE,
        ordType=C,
        ordNo=123456,
        dd=951201,
        tsys=SMS1,
        rsys=sw94sp01,
        userId=PASSWORD,
        aos=AOS,
        version=0x4000000
}
EstRscRec{
        EstChgMovRmvRscRecCtl{
                ctc=B,
                provId=tmpl_cds1
        }
        EstChgRscRecAcl{
                act=N,
                tn=3142319999
                Ains{
                        Tag{
                                TagId=car,
                                TagValue=Y,
                                TagId=car_active,
                                TagValue=N,
                                TagId=car_dmsdid,
                                TagValue=N,
                                TagId=car_dmsdidtrunk,
                                TagValue=00000000,
                                TagId=car_dmsdiddigit,
                                TagValue=7,
                                TagId=car_report1,
                                TagValue=Y,
                                TagId=car_report2,
                                TagValue=Y,
                                TagId=car_adminpin,
                                TagValue=319999
                        }
                }
        }
}
```

SMS Services Impacted:

Edits: The ASID FID/FID data is not provisioned to SPACE. A new column has been added to the FID_ref table called local_only_ind. The value will be 'Y' when a FID's data should be posted to the SMS only and does not provision to a template. When an ASID FID only change is received, Edits should create a Local Only Update. There will not be an associated call variable for the ASID FID in the call variable ref table. Edits should populate the fid_call_variable column in the sav2_fid_call_var table with the value 'NONE.'. Likewise, the FID CARC is a local only FID and will be updated to the SMS only.

POSID will be provisioned on a separate business only template. The only services contained on the template, at this time, will be POSID and DRS. This should be table driven and not result in any coding changes for Edits.

Since the POSID service is sent to the SMS with multiple USOCs, i.e, SCMBX, RS6WX, RU6WX, we originally thought Edits would need to read the USOC_ref table to determine all possible USOCs for a given service and provision as appropriate. The USOC_Group in the USOC_ref table contains a common value for all related USOCs. For example, the USOC_Group should contain the value POSID for all POSID USOCs. Then, when reading the call_variable_ref table, call_variables for all POSID related USOCs would be identified and provisioned. After testing this, it was decided that the SMS will only provision call variables related to USOCs received from SOAC by the SMS. This is because the SMS retains in the customer master view all USOCs provisioned, even if the value associated with the USOC is 'N'. Without further coding, subsequent order activity actually adding a report to POSID failed because the report USOC appeared on the master view (even though the value was 'N'). It appeared that the customer already had the report.

Breakout: As stated in the Edits section, Provisioning to SPACE will not always be necessary. If the ASID FID only is received, a Local Only Update should be created by Breakout. The Local_only_ind in the HOL_step should be set to 'Y' for the given step. If the ASID FID is received in conjunction with other POSID changes or AIN service changes, then Breakout would create a single step with the ASID FID/FID data embedded within the other provisionable changes. As stated previously, the FID/FID data which is local only to the SMS will be designated by the value of 'NONE' in the fid_call_variable column in the save2_fid_call_var.

Provisioning: Provisioning is responsible for rolling the local only updates into the SMS master view. When provisionable changes are included with the local only update (ASID FID or CARC FID), then the data designated as SMS only would be rolled into the master view after successfully provisioning the NE data. If a local only update was sent to the SMS (SOAC activation request only included ASID and no other changes), then the update would be rolled into the master view on the order due date.

GUI: There are eight new phony FIDs: #CAR1 (FID for Access Code screening list), #CM11 (FID for Access Code Comment list), #CAR2 (FID for CPN screening list), #CM21 (FID for CPN comment list), #CM22 (FID for CPN second comment list), #DIGT (FID for DMS DID digit), #TRNK (FID for DMS DID trunk), and #ACTV (FID used for number changes to retain the car_active setting). For provisioning purposes, GUI will need to specify the phony FIDs when updating the associated call variable.

GUI will need to make similar changes like Edits to accommodate multiple USOCs for a given service. For the Order Matrix screen, GUI will read the USOC_ref to determine all available USOCs. However, when more than one USOC is available for a service, GUI will only present one USOC and provide a drop down box for the remaining USOCs. Only USOCs with a USOC_Seq_Num = 1 should be presented on the initial order matrix screen

SPACE Interface: The SPACE Interface will need to recognize FID/FID Data from the STEP tables which does not get provisioned. This can be done be recognizing the value of 'NONE' in the fid_call_variable column.

Data Base: The USOC_Ref and FID_Ref tables have been modified to include the column Local_Only_Ind. Value is Y/N. The ASID FID will be populated with a Y for the Local_Only_Ind in the FID_Ref table as well as the CARC FID. In addition, the USOC_Group_Seq_Num column has been added and will be used to specify the order in which to present the USOCs via the GUI interface. The USOC_Seq_Num will now be used to present the order to present USOCs within a single service. When only a single USOC is used to provision a service, then USOC_Seq_Num will contain a 1. When multiple USOCs are needed to provision a service, then each USOC would contain a unique number (1, 2, 3, etc.).

NOTE: As requirements have not been written for the PC Interface, specific SMS service changes have not been noted.

Reports:

The following data items will be collected by DRS:

Successful Attempts Log Report:	Service Identifier (car) Calling Party Number Called Party Number Date/Time Successful Access Code (if used) Privacy Indicator Report Number (1)
Unsuccessful Attempts Log Report:	Service Identifier (car) Calling Party number Called Party Number Date/Time Unsuccessful Access Code entry Privacy Indicator Report Number (2)

Once all the data is collected by DRS from the ISCP, it will be validated and modified for transmission to the SMS for production of the POSID Reports. The Privacy Indicator will be used by the SMS to determine the value to print on the report for Calling Party Number. Due to privacy issues, the CPN may not always be printed. Or, in some cases the CPN is not available. A value of '00' designates to print full CPN on report; NPA-NXX only for Texas customers. A value of '01' designates to print 'Private' on report in lieu of CPN. And, a value of '10' designates to print 'Unavailable' on report in lieu of CPN. (Note: The 1A on 0.0 AIN software creates a privacy indicator of 99 which means unavailable. Since we are not offering POSID to 1A customers on 0.0, DRS should never create such a sample. To be safe, though, we should code for a Privacy Indicator of 99 to mean Unavailable.) NOTE: the Texas privacy requirement to print only NPA-NXX applies to Texas POSID customer's and their reports only. If a call originates in Texas and is delivered to an Arkansas POSID customer, then the entire NPA/NXX/LINE will be printed.

The SMS will create POSID reports in the same manner we create CID reports. A pull is run against CIDB identifying the customers and their associated report USOCs. As discussed previously in this document, the USOC identifies the report frequency (weekly, monthly). Of course, the SCMBX POSID USOC should be present on the account. The Successful Attempts Log Report is identified by USOC RS6WX (Weekly) or RS6MX (Monthly). The Unsuccessful Attempt Log Report is identified by USOC RU6WX (Weekly) or RU6MX (Monthly). The SMS Customer Report generation software will not read the various SMS tables to identify which reports to create and the report frequency. In addition, the Report Recipient Media and Address RRMA FID will be present on the account in CIDB and is used as the mailing address for the POSID reports. Also, the

media is specified behind the RRMA FID. The Successful Attempts Log Report is available on a floppy diskette only. The Unsuccessful Attempts Log Report is available on paper or a floppy diskette.

Following is an example of the Successful Attempts Log Report:

REDACTED

Positive ID
Successful Attempts Log for NPA/NXX-LINE
mm/dd/yy

Section 1: Calls by Authorized Telephone Number

Calling Number	When Called	
(201) 235-1570	Sun	08:14
		10:22
		15:47
		22:09
	Thu	21:57
	Sat	15:12
	Sun	10:01
		14:57
	Tue	21:17
(201) 235-2135	Sun	20:01
	Sun	19:58
	Sun	19:59
In Texas:		
(201) 235-xxxx	Sun	20:01
(202) 221-xxxx	Sat	08:58

Section 2: Calls by Authorized Access Code

Access Code	When Called		Calling Number
9843	Sun	10:56	(314) 229-6732
1701	Wed	08:17	(201) 480-8700
		13:09	UNAVAILABLE
		20:47	(201) 480-8700
1702	Wed	05:36	(201) 480-8700
		22:21	(201) 480-8700
	Thu	05:47	(201) 480-8700
		13:39	PRIVATE
232916	Fri	08:00	(314) 535-2366
In Texas:			
232916	Fri	08:00	(314) 535-xxxx

Following is an example of the Unsuccessful Attempts Log Report:

REDACTED

Positive ID
Unsuccessful Attempts Log for NPA/NXX-LINE
mm/dd/yy

Calls Not Connected Due to Incorrect Access Code

Calling Number	When Called		Access Code Attempted
(201) 235-1570	Tue	08:14	1000
			1001
		08:15	1002
			1003
		10:22	1004
			1005
	Thu	21:57	356004
(201) 235-2135	Sun	20:01	35670
	Sun	19:58	356700
PRIVATE	Mon	07:38	1238
UNAVAILABLE	Mon	23:01	347838
In Texas:			
(214) 235-xxxx	Tue	11:17	333478
(214) 235-xxxx	Thu	12:38	38784

Profile Management System (PMS):

POSID contains two screening lists: Access Code List (up to 100 rows) and CPN List (up to 500 rows). Due to the size of the lists, DTMF is considered much to cumbersome for customer's to make modifications to the lists with. DTMF update will be allowed, but is intended only for emergency updates. As stated previously, the two screening lists will not be provisioned via service order. This is for two reasons: the large size of the lists, and lack of security if access codes and CPNs are on a service order. The GUI interface is available for provisioning but is intended for problem resolution or emergency updates only. Since the nature of the POSID service is security, customer's want to make their own updates to their lists, without disclosing to anyone the content of their lists. As a result, the Profile Management System (PMS) or PC Interface will be developed allowing customer's with PCs to update their subscription information mechanically.

At the time of this writing, requirements for the PC Interface are in the development stage. At a high level, requirements are as follows:

1. Customers, via their own PC and modem, would dial into the SWBT Profile Management System.
2. Customers would enter a UNIX platform. Currently, CNA appears to be a likely candidate.
3. The customer would be asked to enter a User ID and Password.
4. Once security is verified, the customer would be presented with a list of their services. The customer would specify which service they would like to view or modify.
5. The PC Interface would retrieve the customer subscription information and present to the customer. This is done by submitting a query to the SMS.
6. The customer may then modify their lists. Any edits for the accuracy of the data input would be housed in the UNIX box. Once the customer saves and submits their subscription data modifications, the update is forwarded to the SMS.
7. The SMS would develop a new service to process messages sent from the PC Interface. A separate document has been created containing message formates for all PC/SMS messages.
8. The PC Interface updates sent to the SMS would need to be converted or stored into the PCS data base. Thus, allowing flowthru to provisioning with minor modifications to the SMS.
9. The SMS will be required to send notifications to the PC Interface when Inward or Outward activity occurs on POSID.
10. Customers would not be allowed to add or remove services via the PC Interface at this time.

At this time, there are many unanswered questions regarding the PC Interface. CNA has been identified to support the interface. However, CNA currently only supports the top 250 customers. The number of PC Interface customers could be in the thousands or more. Additional modem resources would need to be secured. In addition, the PC Interface would need 24x7 coverage. CNA provides coverage 7 a.m. to 7 p.m.

REDACTED

The SMS has committed to develop the new interface into the SMS by POSID will be deployed on without the SMS PC Interface. The PC application service will collect Customer subscription data updates and forward to the CNOC for manual provisioning. The SMS will still be required to provision POSID, just without the PC Interface.

Detailed requirements for the Profile Management System (PC Interface) will be documented in a separate requirements document.

P15165.A26

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Paul G. BANIAK et al.	Group Art Unit: 2642
Serial No.	:	09/050,986	Examiner: H. Agdeppa, Jr.
Filed	:	March 31, 1998	
For	:	PROFILE MANAGEMENT SYSTEM INCLUDING USER INTERFACE FOR ACCESSING AND MAINTAINING PROFILE DATA OF USER SUBSCRIBED TELEPHONY SERVICES	

Assistant Commissioner of Patents
Washington, D.C. 20231

DECLARATION OF TERRY L. VIETH PURSUANT TO 37 C.F.R. §1.131

I, Terry L. Vieth, declare that:

1. I am an inventor of the subject matter recited in the claims of U.S. Patent Application No. 09/050,986, currently under final rejection, which claims priority of U.S. Provisional Patent No. 60/042,680. I have personal knowledge of the facts set forth in this declaration.

2. Prior to October 4, 1995, I was a member of a group that was in possession of the profile management system that the Examiner asserts, in multiple Office Actions, is disclosed by Dulman. I know this because prior to October 4, 1995, the group had documented a profile management system that stores profile data on a telecommunications network which executes a telecommunications service subscribed to by a user in accordance with the profile data, the profile management system comprising a client host, a server that processes user requests by obtaining profile data from and forwarding profile data to a

telecommunications network via an intermediate system.

3. Exhibit A is a redacted copy of a document showing work-product of the group (which has been redacted to remove the date). To the best of my knowledge, a date on the original copy of Exhibit A (redacted on the copy provided with this Declaration) was a computer-generated stamp of the date on which the document was created. The date on the document, which has been redacted, is earlier than October 4, 1995.

Exhibit A specifies that a user of the profile management system uses a client host. The user can call a client server which processes user requests to obtain profile data from, and forward profile data to, a telecommunications network via an intermediate system.

4. The project management system was reduced to practice with due diligence from prior to October 4, 1995 to subsequent reduction to practice.

I hereby declare all statements made herein of my own knowledge are true and that all statements made herein on information and belief are believed to be true; and, further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of any issued patent.

Executed: December 17, 2002

Terry L. Vieth

EXHIBIT A

All -

As most of you know, we are in the process of researching a PC Interface that customers can dial into to manipulate their screening lists and customer-specific information related to their AIN products. A new file would then be sent to SMS to be uploaded to the customer's CPR.

In independent exercises, Mike Hanrahan and I both brainstormed about what the screens might look like in order to begin compiling our requirements. Please take a look through these documents and let me know what you think.

A team is quickly gelling and hopefully we will meet in early to officially kick this effort off.

Thanks so much for your time and interest with this!!

Kristin

Kristin Chambers
331-2182

CAR Provisioning

PC Interface - The idea is as follows: Customer, via their own PC and modem, calls into the SWBT "Service Manager." They enter a UNIX platform that is menu driven. The first menu will ask for their USER ID and password. The second menu may ask them to specify which service they would like to update (if this is used for multiple services). They select Computer Access Restriction. There would also be a screen to ask the user if they would like to update their CPNs or their PINs. The system would access a database and bring forward the files associated with this USER ID. If the USER ID is associated with more than one CAR number, then an additional menu would ask the user to specify the account that they would like to update.

The customer has the opportunity to review their list and make any additions or deletions that they would like. Any edits for the accuracy of the data input would be house in the UNIX box, such as validating that a CPN is 10 digits and the Area Code does not begin with 0 or 1. The customer would then save the new file. They are prompted that by saving this file, they will completely overwrite their existing CAR screening lists.

The customer saves the file and the date and time stamp on their file is updated. A 'sweeper' function reviews the date and time stamps on all files on a periodic basis (maybe every 1-10 minutes). When a new date and time stamp is detected, the sweeper picks up the new file and FTPs it to the SMS platform. The SMS platform has a similar sweeper function that looks into a library on a periodic basis and when it finds a new file, it updates the file to SPACE.

SPACE will completely overwrite the existing file with the new file. SMS will have no need to review the files to detect additions or changes, it will just be a complete overlay.

The DTMF would be maintained for turning CAR on and "Checking" CPNs and PINs. The Checker function allows for CPNs and PINs to be added or deleted. Therefore, we would need to create a two-way communication file to relate DTMF updates back to the UNIX platform.

With CAR, it is felt to be a safe assumption that all users will have ready-access to a PC and a modem because of the nature of the service.

Administrative Questions:

Who assigns and maintains USER Ids to the UNIX platform?
How are USER Ids reset in emergencies?
Is there a link between USER Ids and the service order process?
How are new USERs established?
How are disconnected USERs removed?
How is one TN in the USER's profile removed without disconnecting the wholeID?
What hardware is required by the end-user to access the UNIX box?
What organization takes trouble calls?
Who is the administrative support group for the UNIX box?

How is the file sent to SMS?
How is a file received containing DTMF updates?
What is the frequency of the file transfers?
Who maintains a log of those transfers?

Menu Screens and *Functionality*

Log on Screen

```
Enter User ID:
Enter Password:          (prompted after USER ID is input)
```

Validate both the USER ID and password combination. If incorrect, error with the statement "USER ID/Password incorrect." Prompt 2 more times. If a third incorrect entry is input, prompt the customer with "We are sorry. Your USER ID has been deactivated. Please call 1-800-xxx-xxxx to have it reset."

The USER ID should be deactivated after 3 invalid logon attempts. Even if a correct USER ID/password combination are entered, the logon should not be accepted after it has been deactivated. If a user tries to log in following a deactivation, the prompt should read "We are sorry. Your USER ID has been deactivated. Please call 1-800-xxx-xxxx to have it reset," on the first attempt.

The SWBT rep at 1-800-xxx-xxxx should verify some piece of information provided by the customer and reset the password. The default password might be the last four digits of their billing account. (?)

Menu 2

Service Selection Menu

Welcome to Service Management
A service provided by Southwestern Bell

Please select the service that you would like to work with.

_____ Computer Access Restriction

_____ IntelliNumber

_____ Disaster Recovery Service/Intelligent Redirect

_____ Exit

By selecting CAR, the customer is led to the CAR menu options which differ from the others.

Menu 3

CAR Number Selection (optional)

Please select the Computer Access Restriction number that you wish to work with:

_____ (281) 541-1111

_____ (409) 982-6363

_____ (713) 567-8888

To return to previous menu, press 3.

When the customer selects CAR from the previous menu, the UNIX system should query the files and see if there is more than one CAR account associated with this USER ID. If so, the CAR numbers should be retrieved and appear on this menu in numerical order. If not, the customer should skip this screen and advance to the next one.

Menu 4

List Selection

Please select the list that you would like to work with:

_____ Authorized Telephone Numbers

_____ Access Codes

To return to previous menu, press 3.

After the customer selects one or the other the UNIX box should pull up the list requested.

Screen 2

Example of Lists

Authorized Telephone Numbers associated with Computer Access Restriction for (281) 541-1111.

(281) 566-8523
(281) 852-7410
(409) 320-1451
(409) 987-5233
(409) 987-5322
(713) 414-8556
(713) 572-9696
(713) 695-9559

To add new numbers, press 1. To delete numbers, press 2, To return previous menu, press 3, To print, press 5.
Use the Page Up/Down keys to review the entire list.

All numbers are listed by 10 digits, in numerical order.

Menu 5

Number Addition (reached by pressing 1 on previous screen)

```
You have indicated the you would like to add numbers to your
Authorized Telephone Number list for (281) 541-1111.  You
currently have xxx numbers on your list, so you have room
for xx more.

Please type in the number(s) that you would like to add:

(xxx)  xxx-xxxx
(xxx)  xxx-xxxx
(xxx)  xxx-xxxx
(xxx)  xxx-xxxx
(xxx)  xxx-xxxx
(xxx)  xxx-xxxx

Press 1 to add these numbers, press 2 to return to the
Authorized Number list.
```

When the Addition menu is accessed, the UNIX platform needs to read the existing file and report on the screen how many numbers on currently on the list and how many are remaining (200-existing numbers). Space should only be provided for the number of numbers that can be added. For example, if the customer only have 10 spaces (list contain 190 numbers already) then only 10 blanks should be provided. If the customer has over 20 numbers remaining, provide spaces in blocks of 20. In other, ask for the confirmation prompt after 20 numbers.

Within the number spaces, all arrow keys and number keys should work. Customer should be able to tab to the next number and shift-tab back a number, as well as use the arrow keys. Any number can be edited while on this menu.

If they press 1 to accept these additions, the following edits should be administered:
Check to see if number is 10 digits
If so, return addition screen with number highlighted and the error message printed at the bottom reading "Authorized Telephone Numbers must be 10 digits."

Check to see if NPA begin with a 0 or 1
If so, return addition screen with number highlighted and the error message printed at the bottom reading "Area Code cannot begin with a 0 or 1"

Check to see if number is already on list
If so, return addition screen with number highlighted and the error message printed at the bottom reading "This number is already on the Authorized Telephone Number list"

Edits should be performed as all numbers for error condition 1, error screen, then all numbers for error condition 2 then the error screen, etc. This way, multiple numbers can be highlighted with the same error condition.

Screen 3

```
Numbers Added

Press 1 to add more numbers
Press 2 to review new Authorized Telephone Number List
```

If 1, return to menu 5
If 2, go to screen 4.

Screen 4

Example of Lists

```
Authorized Telephone Numbers associated with Computer Access
Restriction for (281) 541-1111.

(281) 566-8523
(281) 852-7410
(281) 987-5874
(409) 320-1451
(409) 987-5233
(409) 987-5322
(409) 989-1010
(713) 414-8556
(713) 565-9630
(713) 572-9696
(713) 695-9559

To Save new list, press 4,  To add new numbers, press 1.  To
delete numbers, press 2, To return previous menu, press 3,
To print, press 5.
Use the Page Up/Down keys to review the entire list.
```

If list has changed from saved version (additions or deletions made), add highlighted prompt to save new list.

Menu 6

Save Confirmation

You have indicated that you would like to save a new Authorized Telephone Number List. Please note the saving this list will completely overlay your previous one.

Press Y to confirm the new list.
Press N to return to the Authorized Telephone Number List ,

Menu 7

Following Save Confirmation

Your new Authorized Telephone Number List has been saved.

Please choose your next option:

_____ Return to List Selection
Authorized Telephone Numbers or
Access Codes

_____ Return to CAR Telephone Number Selection

_____ Return to Service Selection
Computer Access Restriction
IntelliNumber
Disaster Recovery Service/Intelligent Redirect

_____ Exit

Screen 5

Following Exit

Thank you for using the Southwestern Bell Service Manager

Any changes should be updated within the next 2 hours.

Please call 1-800-xxx-xxxx if you had any difficulty with this system.

The same type of functions would be available to delete CPNs, add/delete PINs.

P15165.A31

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Paul G. BANIAK et al.	Group Art Unit: 2642
Serial No.	:	09/050,986	Examiner: H. Agdeppa, Jr.
Filed	:	March 31, 1998	
For	:	PROFILE MANAGEMENT SYSTEM INCLUDING USER INTERFACE FOR ACCESSING AND MAINTAINING PROFILE DATA OF USER SUBSCRIBED TELEPHONY SERVICES	

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313

SUPPLEMENTAL DECLARATION OF TERRY L. VIETH PURSUANT TO 37 C.F.R. §1.131

I, Terry L. Vieth, declare that:

1. I am an inventor of the subject matter recited in the claims of U.S. Patent Application No. 09/050,986, currently under final rejection, which claims priority of U.S. Provisional Patent No. 60/042,680. I have personal knowledge of the facts set forth in this declaration.

2. I have previously executed a Declaration of Terry L. Vieth pursuant to 37 C.F.R. §1.131 on December 17, 2002, and incorporate this Declaration by reference herein.

3. From prior to October 4, 1995, I was a member of a group that was in possession of the profile management system that the Examiner asserts is disclosed by Dulman. From prior to October 4, 1995 (i.e., prior to the filing date of DULMAN) the group worked diligently until the profile management system was reduced to practice.

4. Exhibit A is a screen-shot of a website showing a reduction to practice of the profile management system. Exhibit A is a press release announcing the availability of the profile management system in Austin, Texas. The press release is entitled 'Southwestern Bell Introduces "Padlock" for PCs' and is dated April 5, 1996. To the best of my knowledge, the press release was downloaded from the internet at <http://www01.sbc.com/About/NewsCenter/ShowRelease/1,,38,00.html?NID=1996> on May 22, 2003.

5. I have personal knowledge of efforts to reduce the profile management system to practice from before October 4, 1995 (i.e., the filing date of DULMAN) until the profile management system was reduced to practice. I have personal knowledge of activities of the group, including multiple meetings of members of the group and timelines of tasks assigned to members of the group, from before October 4, 1995 until the subsequent reduction to practice. The meetings and timelines include dates of activity starting before October 4, 1995 and diligently continuing until the subsequent reduction to practice.

I hereby declare all statements made herein of my own knowledge are true and that all statements made herein on information and belief are believed to be true; and, further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of any issued patent.

Executed on: 8-11-3

Terry L. Vieth

EXHIBIT A

SBC Home
My Account
Residential Products and Services
Business Products and Services
Repair
Billing and Account
Site Search
SEARCH
SMARTpages™ White and Yellow Pages
Site Map
FAQs
Contact Us
Get Email Updates
Manage your subscription for news, tips and promotions.
Enter Email Address
GO!

News Center

Southwestern Bell Introduces "Padlock" for PCs

Positive ID Responds To Growing Need To Safeguard Computer And Voice Networks Of Medium, Large Businesses

St. Louis, Missouri, April 05, 1996

Southwestern Bell is introducing a "PC padlock" that helps businesses shielc their computer networks from "hackers."

Positive ID, a new service Southwestern Bell will introduce in Austin, Texas, designed for businesses that provide dial-up access to their computer networks. The new service allows users to authorize incoming calls for acce: to computer terminals and other devices and denies unauthorized calls and callers without an access code.

The rise of Internet, SOHO (small office/home office) market and telecommuting applications have required workers to access computers fror outside the office, fueling the need for dial-up access to company database: and corporate computer networks.

A recent study by the National Computer Security Association (NCSA) founc that 34 percent of surveyed companies suffered break-ins, while 11 percent could not even determine if their system had been breached. The study alsc revealed that companies providing Internet access to and from their networ were eight times as likely to suffer break-ins.

"Computer authorization systems like Positive ID are the first line of defens against hackers who dial into corporate networks, a practice that costs corporations nearly $1 billion annually," said Michelle Watson-Williams, marketing manager for Southwestern Bell.

PBX systems that allow access from remote locations also are vulnerable to fraud. The International Communications Association estimates that toll frai costs corporations nationwide between $500 million and $6 billion annually.

"With Positive ID, we are meeting the growing need for computer and PBX network security by our customers," said Watson-Williams.

While Southwestern Bell manages the operational features of Positive ID, companies' network administrators control access codes, authorization modification and security monitoring. Network managers and MIS directors even have the ability to review access attempts over a period of time, allow

them to more effectively manage security efforts.

Companies can identify up to 500 authorized 10-digit telephone numbers ar 100 authorized four- to seven-digit access codes for each network terminal device. Positive ID's Interactive Voice Response (IVR) feature enables netw managers and MIS directors to monitor active authorization codes or phone numbers and to instantly change those codes. Reports, available weekly or monthly on paper or diskette, display the date, time, area code and prefix c any caller attempting to access a company's network.

"Monitoring system access attempts is an important step to preventing brea ins," added Watson-Williams. "Southwestern Bell's Positive ID gives busines an exceptional level of control over their network."

Unlike other security systems, Positive ID requires no additional hardware, software or staffing, providing a great value to businesses. Southwestern B Advanced Intelligence Network (AIN), an infrastructure enhancement to the regular phone network, is the foundation of the service.

The central computer database -- the 'intelligent' part of the new technolog is the key to AIN. With AIN, Southwestern Bell creates cost-effective, call-management services and tailors them to fit the individual needs of its customers. New services such as Positive ID allow businesses to maximize resources by getting the most out of their telephone and computer network and improving customer service.

For more information about Positive ID, or to order the service, call toll-free 1-800-234-BELL.

# # #

SBC Communications Inc. is one of the world's leading diversified telecommunications companies and the second largest wireless communications company based in the United States. SBC provides innovat telecommunications products and services under the Southwestern Bell and Cellular One brands; wireless services and equipment in the United States a interests in wireless businesses in Europe, Latin America, South Africa and Asia; cable television in both domestic and international markets; and direc advertising and publishing.

Positive ID Fact Sheet

Hackers who dial into corporate networks cost corporations nearly $1 billion annually.

National Computer Security Association (NCSA) Study Results

- *Companies providing Internet access to and from their networks are eight times as likely to suffer break-ins.*
- 34 percent of the companies surveyed suffered network break-ins.
- 11 percent of the companies surveyed could not even say if their syst

had been breached.

PBX Fraud

- *Consultants estimate that one in 18 hackers attempt to gain illicit ent into a corporation's PBX system.*
- If a phone system allows users to dial out from a remote location, the system is vulnerable.
- The International Communications Association estimates that toll frau costs corporations nationwide **between $500 million and $6 billior annually.**

Southwestern Bell's Positive ID

- Positive ID, a service based on advanced intelligent network technolo *allows businesses to authorize incoming calls for dial-up access to computer terminals, PBX systems and other devices, and to deny unauthorized calls and callers without an access code.*
- Companies can identify up to 500 authorized 10-digit telephone numt and 100 authorized four- to seven-digit access codes for each networl terminal or device.
- Network managers and/or MIS directors can monitor call volume into their company's communications devices; act as security managers b reviewing access attempts over a desired period of time; and instantl change authorization codes by dialing the Interactive Voice Response system.
- Reports, available weekly or monthly on paper or diskette, display the date, time, area code and prefix of any caller attempting to access a company's network.

- For more information about Positive ID, or to order the service, conta 1-800-234-BELL.
